Australian Government
Department of Defence
Defence Science and
Technology Organisation

Technical Risk Assessment: a Practitioner's Guide

John O'Neill, Nitin Thakur and Alan Duus

Defence Systems Analysis Division
Defence Science and Technology Organisation

DSTO-GD-0493

ABSTRACT (U)

DSTO's formal process of preparing Technical Risk Assessments (TRA) for Projects has been in operation for several years. A recent review of TRAs conducted by Studies Guidance Group revealed the high value-add from DSTO TRAs is in identifying integration risks, and also showed some weaknesses in identifying and assessing System Readiness Levels and identifying technical risks. This paper supplements DSTO's existing TRA guidance by: 1) focusing on how to identify and assess System Readiness Levels; 2) articulating the difference between technological risk and technical risk; and 3) suggesting sets of candidate technical risks that may be relevant to ADF projects.

RELEASE LIMITATION

Approved for public release

Published by

Defence Systems Analysis Division
Defence Science and Technology Organisation
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR-013-821
February 2007

Conditions of Release and Disposal

Technical Risk Assessment: a Practitioner's Guide

Executive Summary

The Defence Procurement Review recommended that acquisition projects should be subject to comprehensive assessment of technology risk. DSTO has instituted processes for undertaking these assessments, and these have been in place for several years.

A recent review by Studies Guidance Group of the quality of the Technical Risk Assessments that have been certified by the Chief Defence Scientist found strengths and weaknesses in the current approach. In particular, the review found:

1. that the major value added to the project and senior Defence committees by the DSTO technical risk assessment process is the identification of integration risks and dependencies, particularly across projects;

2. that the identification of technologies for a project and an assessment of the maturity of the technologies – the Technology Readiness Level - is working well;

3. that the identification and assessment of System Readiness Level is more problematic;

4. that there is still confusion about the differences between technology risk and technical risk;

5. that the process for the identification of a set of candidate technical risks for a project is not well understood;

6. that there are opportunities at the Options Review Committee for preliminary technical risk assessments to play a greater role in shaping the project and the analytical and risk mitigation work conducted in support of that project;

7. that the technical risk assessment needs to be considered within the 'context of use'. The context of use is normally defined in the Operational Concept Document and Functional Performance Specification. If the context of use is not defined then the technical risks cannot be assessed and the overall technical risk defaults to HIGH;

8. that the Chief Defence Scientist has directed that he will not certify any statements about predictions of future technical risk or mitigated risk. While the Chief Defence Scientist expects statements about possible risk mitigation strategies in the TRA, he will only certify the technical risk at the current time; and

9. that TRAs should be published as DSTO Client Reports.

This paper re-iterates the distinction between technology risk and technical risk as defined in [4]. *Technology Risk* is the likelihood that an underpinning technology necessary for a capability will not mature within the required timeframe. *Technical Risk* is the likelihood that the system will not reach its goals for performance, cost or schedule due to technology risks, to risks which arise in the integration of critical technologies and/or sub-systems dependent on them, or to the system integration into the ADF Using these definitions it is clear that many of the TRAs conducted to date have focussed on the technology risks and have not included the broader set of technical risks. For example, in acquiring a system in operational use in the US there are unlikely to be any technology risks. But there may be technical risks for operating in the Australian context due to differences in Australia's operating environment (heat, humidity), differences in the ADF C4ISREW system, differences in the way Australia operates the platform, differences in the through-life support requirements and life-of-type for the platform in the Australian context.

This paper addresses the findings of the review by providing additional guidance to practitioners (generally Project S&T Advisers) in the following areas:

1. establishing the 'context of use';

2. identifying the system boundary;

3. identifying the key sub-systems for each option;

4. identifying the technologies which need to be delivered for each sub-system to work;

5. identifying which DSTO divisions (and other areas) should be involved and organise a TRA workshop;

6. evaluating the maturity of each technology, expressing the result using TRLs;

7. evaluating the maturity of each sub-system, expressing the result using SRLs;

8. identifying the set of candidate technical risks for the project;

9. assessing the technical risks for the project;

10. identifying possible risk mitigation strategies and incorporate into the Project S&T Plan; and

11. identify strategic issues related to the Project.

Where appropriate, there are series of questions to help guide the practitioner through the process. In particular, this report clarifies the difference between technology risk and technical risk, and identifies sets of technical risk events that are relevant to Defence projects. These technical risk events are related to increasing the maturity of individual technologies, and will be different for developmental and acquisition strategy projects, platform projects, and the software component of projects. Many

projects include aspects of each of these project types, and it would be expected that the Project S&T Adviser would use this approach to assist in identifying a candidate set of technical risks for the project.

The differing nature of the technical risk assessment is discussed at three important stages in the development of a project during the Requirements Phase – Options Review Committee consideration prior to first pass; at first pass; and at second pass.

Finally, there is a discussion about the relationship between TRAs and studies, and the feedback loops in both directions.

Authors

John O'Neill
Defence Systems Analysis Division

Dr O'Neill is currently Head, Studies Guidance Group. He has a PhD in Computer Science and has conducted research into C2 systems for Defence, NASA and United Airlines. His research interests include the strategic implications of technology and the emerging applications of technology.

Nitin Thakur
Defence Systems Analysis Division

Dr Thakur joined Defence after a Post Doctoral stint in Nuclear Physics, Australian National University, and a degree in Management Science. He worked in Science Policy Division, DSTO, for a while; later moved to Defence Systems Analysis Division, supporting a range of studies such as the ADF Lift Study and Preparedness; and currently works in Studies Guidance Group.

Alan Duus
Defence Systems Analysis Division

Dr Duus graduated from the Australian National University with a Ph.D in Astronomy. He joined Central Studies Establishment of the Defence Science and Technology Organisation and contributed to Operations Analysis of a range of Defence issues. Following a series of postings within Defence and overseas, he led the DSTO support to the AEW&C Project from its inception to contract signature. He resigned from Defence in 2001, and contributed to this work as a consultant.

Table of Contents

List of Abbreviations

ADF	Australian Defence Force
Cabsub	Cabinet Submission
CDS	Chief Defence Scientist
DCC	Defence Capability Committee
DCIC	Defence Capability Investment Committee
DGPG	Director General Planning and Guidance
DPR	Defence Procurement Review
DSAD	Defence Systems Analysis Division
DSTO	Defence Science and Technology Organisation
FPS	Functional Performance Specification
HSGG	Head, Studies Guidance Group
OCD	Operational Concept Document
OR	Operations Research
ORC	Options Review Committee
SA-CD	Scientific Advisor, Capability Development
SGG	Studies Guidance Group
SRL	System Readiness Level
TEP	Test and Evaluation Plan
TRA	Technical Risk Assessment
TRL	Technology Readiness Level
WBS	Work Breakdown Structure

1. Background

The Defence Procurement Review [1] was undertaken to address perceived deficiencies in the Defence acquisition processes. One of the Review's recommendations was that the Chief Defence Scientist (CDS) would be responsible to Government for assessing and certifying the technical risk for projects at first and second pass.

As part of the Defence Science and Technology (DSTO) response to the review, DSTO has:

1. appointed a DSTO Project S&T Adviser for each project [2];

2. developed policy for the undertaking of Technical Risk Assessments (TRAs) [3], [4];

3. developed guidance and assistance for preparing Project S&T Plans [2], [5] and [6];

4. developed pro-formas for preparing Project S&T Plans and training packages for Project S&T Advisers[1];

5. conducted over 60 TRAs; and

6. certified over 60 TRAs for projects at first and second pass (this certification is effected by CDS's signing a technical risk certification minute stating his evalution of the technical risk statement in the Cabsub advised by the TRA, as recommended in [1]).

Studies Guidance Group (SGG) of the Defence Systems Analysis Division (DSAD) is responsible for the development of policy for the preparation of TRAs, facilitating the implementation of the TRAs, and conducting the technical risk certification process for CDS. SGG has reviewed the TRAs that have been certified by CDS. The key findings of the review are:

1. that the major value added to the project and senior Defence committees by the DSTO TRA process is the identification of integration risks and dependencies, particularly across projects;

2. that the identification of technologies for a project and an assessment of the maturity of the technologies – the Technology Readiness Level (TRL) - is working well;

3. that the identification and assessment of System Readiness Level (SRL) is more problematic;

[1] Policy, pro-formas, and training packages for Project S&T Advisers can be found at http://web-vic.dsto.defence.gov.au/DSTO/reference/DPR/index.shtml

4. that there is still confusion about the differences between technology risk and technical risk;

5. that the process for the identification of a set of candidate technical risks for a project is not well understood;

6. that there are opportunities at the Options Review Committee (ORC) [6] for preliminary TRAs to play a greater role in shaping the project and the analytical and risk mitigation work conducted in support of that project;

7. that any TRA needs to be considered against the 'context of use'. The context of use is normally defined in the Operational Concept Document (OCD) and Functional Performance Specification (FPS). If the context of use is not defined then the technical risks cannot be assessed and the overall technical risk defaults to HIGH;

8. that CDS has directed that he will not certify any statements about predictions of future technical risk or mitigated risk. While CDS expects statements about possible risk mitigation strategies in the TRA, DSTO cannot guarantee the future level of technical risk as a result of implementing these strategies. Therefore, CDS will only certify the technical risk at the current time; and

9. that TRAs should be published as DSTO Client Reports.

2. Aim

This document builds on the original TRA Tiger Team work [3], [4] to address the issues identified in the review above[2]. Specifically, this document aims to provide guidance to Project S&T Advisers in identifying and assessing SRLs and identifying and assessing technical risks. In parallel, a new pro-forma for ORC TRAs has been constructed and the pro-formas for First Pass and Second Pass TRAs have been updated to reflect the lessons learned, content of this document, and to facilitate publication as DSTO Client Reports[3].

3. Conducting a Technical Risk Assessment

Preparing a TRA involves using a structured thought process that takes a systems perspective. It starts with an understanding of how the system is proposed to be used in the Australian Defence Force (ADF) and of the sub-systems involved. The steps in this process are:

---

[2] SGG provides TRA training on a regular basis at all major sites. The training material is available at http://web-vic.dsto.defence.gov.au/DSTO/reference/DPR/index.shtml. Please contact HSGG for further information.

[3] The new pro-formas are available at http://web-vic.dsto.defence.gov.au/DSTO/reference/DPR/index.shtml or contact HSGG.

1. establish the 'context of use';

2. identify the system boundary;

3. identify the key sub-systems for each option;

4. identify the technologies which need to be delivered for each sub-system to work;

5. identify which DSTO divisions (and other areas) should be involved and organise a TRA workshop;

6. evaluate the maturity of each technology, expressing the result using TRLs;

7. evaluate the maturity of each sub-system, expressing the result using SRLs;

8. identify the set of candidate technical risks for the project;

9. assess the technical risks for the project;

10. identifying possible risk mitigation strategies and incorporate into the Project S&T Plan; and

11. identify strategic issues related to the Project.

While this may appear to be a linear process, in practice it is recursive. The points of recursion may include:

1. The need to develop a (draft) TRA for ORC that identifies high risk / high payoff areas for further study and development, and fully developed TRAs for first and second pass;

2. As steps 6-10 are conducted, it is highly likely that issues will emerge that will require additional work in the earlier steps; and

3. The project options are likely to change, particularly between ORC and first pass. The options can change between DCC/DCIC and the Cabsub, which may require a quick reassessment of the technical risks.

3.1 Establish the 'context of use'

The 'context of use' establishes the ADF requirement for use of the system. This context will evolve as the project matures as follows:

1. at project inception, the context of use is the statement of capability need;

2. as the project evolves, the development and refinement of the OCD and FPS will provide the detailed context of use that will provide the necessary background and permit the assessment of the technical risks for a project;

3. the tender evaluation will provide the detailed technical information required to complete the second pass TRA; and

4. for pre-Kinnaird Projects, a simple concept of employment may need to be developed (there are very few Projects in this category in 2007).

If the context of use is not defined then the technical risks cannot be assessed and the overall technical risk defaults to HIGH.

3.2 Identify the system boundary

The system boundary for the project is established from the context of use. In particular:

1. what exists inside the system boundary (i.e. within the project scope);

2. what are the entities that cross the system boundary both to the project and from the project; and

3. for the entities that cross the systems boundary, where do they come from and where do they go to (i.e. to other projects or legacy systems).

Entities that cross the system boundary might include:

1. information flows (message sets);

2. communication dependencies (networks and interfaces);

3. physical space dependencies (physical size and weight);

4. command and control dependencies (nexus with other command and control systems); and

5. logistics dependencies (assumptions about the ability of other capabilities to deliver required fuel, stores etc).

Identification of the system boundary and the entities that cross the system boundary is a key issue for the Project S&T Adviser because:

1. it identifies other projects (if any) that may share integration risks with this project;

2. it assists in identifying other Project S&T Advisers who will need to be involved in developing the TRA; and

3. it shifts the focus for identifying the key sub-systems away from a purely project focus to understanding the connection of these sub-systems into the larger ADF.

3.3 Identify the key sub-systems for each option

Having established the context of use, system boundary, and the entities that cross the system boundary, the next step is to identify the key sub-systems for each of the specified options.

There are different approaches to identifying the key sub-systems depending on the type of project and the progression of the project in the capability development process [6]. Some approaches include:

1. a work breakdown structure (WBS) or functional perspective that breaks the project down into components and identify the requirements each component needs to address - for example, a platform may require propulsion, structure, sensors, weapons, load space, C2, crew compartments etc; and

2. a development perspective - for example, software projects at first pass often have option sets defined in terms of different development strategies (buy COTS components, evolve the extant system, develop new system from scratch). Key issues from a sub-systems perspective involve identifying the relevant architectures and interfaces both within the project and in the larger ADF context.

An area of 'missed risks' that was identified in the SGG review is that the definition of the sub-systems using the WBS perspective often takes only an inward looking project perspective. The sub-system view needs to be expanded to include those entities that cross the system boundary (as articulated in Section 3.2).

3.4 Identify the technologies which need to be delivered for each sub-system to work

For each of the sub-systems, list the technologies that are required to enable that sub-system to work.

3.5 Identify which DSTO Divisions (and other areas) should be involved and organise a TRA workshop

Most Projects involve a range of systems and technologies. As such, there are very few Pre-Second Pass projects where all the DSTO support comes from a single Division. Multi-divisional support to projects is the norm and one of the key roles for a Project S&T Adviser is coordinating this multi-divisional support.

In preparing the TRA, the Project S&T Adviser should look at engaging other Divisions (and other areas) based on the following:

1. identification of technologies and Operations Research (different Divisions in DSTO are responsible for different technologies or support different operational environments); and

2. identification of related projects (it is likely that the Project S&T Advisers for some of these other projects will be in other Divisions)

There are a couple of points to note in regarding engaging other Divisions (and other areas):

a) while CDS expects the Project S&T Adviser to be the single DSTO point of contact for the project, CDS does not expect the Project S&T Adviser to be the expert in each of the technical areas for the project. Rather, CDS expects the Project S&T Advisor to leverage other technical experts across DSTO and to seek expert advice from outside DSTO if required; and

b) where the Project S&T Adviser is experiencing difficulty engaging other Divisions, the Project S&T Adviser should first seek the assistance of their Research Leader and Chief of Division in establishing the appropriate relationships. If the engagement is still unsuccessful, the Project S&T Adviser should contact HSGG or SA-CD.

Having identified the relevant technologies and relevant expertise, the Project S&T Adviser is strongly encouraged to run a TRA Workshop specifically relevant to that project. This will need to include the DSTO subject matter experts contributing to the project, and SGG should be involved to ensure TRAs will meet CDS's technical risk certification requirements.

3.6 Evaluate the maturity of each technology

DSTO uses the TRLs [4] as the basis for assessing the maturity of the technologies. For each technology, the current maturity of the technology is expressed as a number and is supported by a short sentence explaining the rationale behind that assessment.

The TRL needs to be evaluated in the specific context of both the context of use and the proposed solution. It should not be a generic statement about the technology. For example:

- radar technology is a well established technology and rates a TRL of 9
- but the specific radar proposed for a specific system may only have a TRL of 3
- there may have been a demonstration (TRL 6-7)
- but if the number or scope of the changes from that demonstrated is large then the TRL is 3

It is not appropriate to describe the maturity of the technology as a wide range, for example, TRL 2-8. In situations where the maturity of the technology appears to fit a wide range, then either:

1. DSTO does not have a good understanding of the current maturity of the technology (and the assessment should be accompanied by a suitable caveat); or

2. there is a blurring between what is generally available versus what is specifically available to meet the requirement; or

3. the technology descriptor is actually covering a number of technologies at different maturity levels. In this case, it is more useful if the technology is described at a lower sub-system level thus providing a better understanding of the maturity of each technology.

This section should also refer to the set of studies that provided the technical basis for the assessment of TRLs.

An example of the TRL summary table is shown in Table 1 below.

Table 1. Example TRLs

Technology Example	Estimated Readiness Level	Comments
Hardware suite for ADF Deployable Logistic System (ADFDLS)	5-6	JP 2077 progressing development of ADFDLS software applications hosted by this JP 126 provided hardware.
Centre Barrel Replacement Line	7	USN have performed a number of Centre Barrel Replacements on their aircraft. A Line has not yet been setup in Australia to refurbish RAAF F/A-18s.
Intranet (web) browsing Guard	6-7	Under NSA evaluation DSTO is currently unable to confirm this level of maturity for web browsing guards.

3.7 Evaluate the maturity of each sub-system

By following the structured thought process outlined in this paper, the Project S&T Adviser should have a list of the sub-systems, a list of the technologies for each sub-system, and an assessment of the maturity of each technology.

The next step is to put this information together to evaluate the maturity of each sub-system, expressing the results in terms of SRLs [4]. Evaluating the SRLs requires:

1. understanding the maturity of each of the individual technologies;

2. understanding the entities that cross the system boundary;

3. understanding the maturity of the process of integrating these technologies together into the required sub-system;

4. understanding from the WBS requirements how much work is required for this sub-system to meet the requirement; and

5. noting that the level of detail required to evaluate the SRLs often only emerges in the response to the tender process that occurs between first and second pass. The Project S&T Adviser must be involved in the tender evaluation process in order to be well-positioned to evaluate the maturity of SRLs.

It is possible to have a set of mature technologies at the TRL 9 level that have never been integrated before into the ADF, resulting in a low SRL. There are potentially issues in almost every aspect of the integration of a new system, since the final design is often a trade-off across several dimensions. A system configured for one particular purpose might not necessarily work in the proposed set-up for physical, electronic, electromagnetic, communications architecture or human machine interface reasons.

An example of a summary table is shown in Table 2 below.

Table 2. Example showing SRLs

Sub-system Example	Technologies for each sub-system	Technology Readiness Level	System Readiness Level	Comments
Incorporate wireless LAN for BCSS	xxx	5-6	4	
	yyy	7-8		
Missile System and technologies	Target Acquisition	8	8	
	Datalink	8		
	Propulsion	9		
Mission System Integration	Mission data requirements	6-7	6	
	Real time updates	6-7		

3.8 Identify the set of candidate technical risk events for the project

Many of the TRAs reviewed by SGG have focused on identifying the technical risks in increasing the maturity of technologies from their current level to a TRL of 9. While this is one type of technical risk event, it does not constitute a complete set. Understanding why it is an incomplete set requires a re-examination of the definitions of technology risk and technical risk outline in [4].

> *Technology Risk*. The likelihood that an underpinning technology necessary for a capability will not mature within the required timeframe.
>
> *Technical Risk*. The likelihood that the system will not reach its goals for capability performance, cost or schedule due to technology risks, to risks which arise in the integration of critical technologies and/or sub-systems dependent on them, or to the system integration into the ADF.

This section documents additional categories of technical risk events that may apply to Defence projects. These have been listed in terms of development projects and acquisition strategy issues, platform project and the software component of project issues, although it is likely that any given project will draw technical risk events from each of these categories.

3.8.1 A development project / acquisition strategy issues

1. Is the proposal technically sound? Will the technology work as specified in the required timeframe? Is the maturity of the technology a time and money issue, are there fundamental research breakthroughs required, or are there scaling or architectural issues?;

2. What confidence do we have that the project will run to completion? Does the contractor have the resources and expertise to successfully deliver the project?;

3. If the project relies on a technology process (eg structural refurbishment), what confidence do we have that the Australian contractor will be able to run the technology process to completion? What confidence do we have that the technology process will take the same amount of time when conducted by an Australian contractor on ADF platforms (with potential different fatigue issues) compared with similar overseas processes? What is the impact on capability and schedule as a consequence of any uncertainty with the implementation of this technology process?[4]

4. Are there any technical reasons why the proposal will not meet Australian capability requirements?;

5. What are the integration risks for this proposal working in the Australian environment?;

6. Are there any certification issues involved in this proposal? Will Australia be accepting the "first of type" and if so what issues need to be addressed? What is the tradeoff between moving down the production line and allowing another country to bear many of the certification risks versus the delays into service from a capability perspective?

7. What regulatory hurdles need to be addressed before the project is successfully accepted into service (RF emission licenses, ship MARPOL regulations, airworthiness certifications)?

8. Have the 'right' technologies been locked in from a strategic perspective? By going down this particular technology path: a) has the ADO locked itself out of a competing technology; b) created longer-term support issues, such as increasing the cost of upgrades;

9. What are the implications for DSTO's S&T support base? What risk mitigation work does DSTO need to conduct up to acceptance into service testing? What through-life support will DSTO need to conduct for this project and what infrastructure and skill base will be required, for example, fatigue testing, development of tactics and doctrine, technology insertion for future upgrades?; and

10. Are there any consequences derived from the acquisition strategy? The contract will address the relationship between the prime contractor and individual sub-contractors. Responsibility for the development of different sub-systems might lie with different sub-contractors, and integration of these into the system might be the responsibility of another. The Project S&T Adviser should be fully aware of these arrangements, and of the consequences for the assessment of technical risk. The proposed risk mitigation strategies might also vary from one possible prime contractor to another.

[4] For example, AIR5376 Ph3.2 Centre-Barrel Replacement on F18s was employing a technology process successfully used overseas, but we were uncertain how many hours it would take on Australian F18s because of their different fatigue issues.

3.8.2 A platform project

1. What are the integration issues onto the platform including power, physical space, weight, heating, cooling, integration into existing data buses, information sharing, mission systems, electro-magnetic interference? Is there anything unique in this particular integration that might constitute a significant technical risk event?;

2. What are the human systems aspects of the proposal? These aspects may include changes to data display screens, ability to process information, physical space issues in crew compartments;

3. What are the cumulative effects on the overall platform as a result of these integration issues (for example, is the platform now overweight, short on power, at the limits of its CPU capacity)? Has the platform exceeded any design limitations, and if so, what is the impact?;

4. Which sub-systems will need to be upgraded in what timeframes? Do the new sub-systems being integrated impact on the planned upgrade schedule (either positively or negatively)? Are there supportability issues emerging for any of the sub-systems?; and

5. How have the dependencies (cross system boundary flows) changed between this platform and the wider Defence environment as a result of this proposal?

3.8.3 The software component of a project

1. What is the software architecture? How does this architecture integrate into the broader Defence Information Environment?;

2. What are the capacity issues for this software in terms of CPU requirements, memory requirements, storage requirements, network requirements? How do these capacity issues impact on other software projects? Will the current system software and application software support this new software or are upgrades required? If upgrades are required what other software projects are affected?;

3. Will the current hardware environment support this software (hardware obsolescence management issues)? Hardware includes the computer system including all input and output devices;

4. What is the growth capacity for the software? Software systems are designed to handle a number of transactions per minute. What happens if the number of transactions doubles, triples or increases by an order of magnitude? Alternatively, how easy is it to add new functionality to the software and what is the impact? In both cases, the impact must be assessed not only in terms of the software architecture but the capacity issues listed above;

5. Are there any Intellectual Property issues?; and

6. Is there sufficient technical expertise to: a) develop the software; b) to support the software system for its life of type; and c) to maintain and update the software. A key point is that the technical expertise is different for each of these issues.

3.9 Assess the technical risks for the project

3.9.1 The technical risk assessment for each technical risk event

Having identified a candidate set of technical risks for the project, an assessment of the technical risks is then conducted using the likelihood versus consequence approach outlined in [4]. The consequence should be assessed in terms of the importance of achieving the required capability.

The technical risks for the project should be presented as a summary table with an assessment of the overall technical risk for the project as shown in Table 3 below.

Table 3. Technical risk assessment at second pass.

Key technical risk areas		**Option 1**	**Option 2**
Will program succeed technically?			
	Weight Growth	L	L
	Airframe and Engine Life	M	L
	Control system effectiveness	M	L
	Store release clearances	L	L
	Inadequate sensor performance	H	L
Will it work as a system?			
	Lack of national infrastructure	H	H
	Lack of training system environment	H	H
Will it be supportable through LOT?			
	Availability of technical information	M	L
	Reserve capacity	M	L
Overall Technical Risk		M-H	L-M

3.9.2 Assessment of the overall TRA – how to aggregate technical risks

There are a number of different methods for aggregating the overall technical risks:

1. The highest technical risk assessment drives the overall technical risk for the project. This is often the case for projects requiring extensive integration and in which the integration risk is the highest risk;

2. Identify the technical risks that are 'core' to the system and aggregate the risks across those components (noting that the TRA is not an exhaustive list of all technical risks in that many LOW risks may not be recorded);

3. Some projects are a loose collection of components. Instead of an overall technical risk, a better approach is to identify the technical risks of the 2-3 major components.

3.10 Identify possible risk mitigation/management strategies and incorporate into the Project S&T Plan

The key issue for senior decision makers is what to do about the technical risks, with particular focus on the HIGH and MEDIUM technical risks. Risk mitigation strategies should be developed at least for each of the HIGH and MEDIUM technical risks. There may be some risks that cannot be mitigated because the development program is outside Australia's control. For these risks, we need to outline how we would manage the risk, for example, putting a technical liaison officer into the overseas development areas.

CDS is particularly interested in a statement of the confidence that DSTO has that these risk mitigation strategies will transform one risk to another risk (which is then assessed as having a lower risk).

The risk mitigation and risk management strategies will need to be transferred to the Project S&T Plan with appropriate costing and resourcing data to enable senior defence committees to make decisions about which risk mitigation strategies should be funded. Types of risk mitigation DSTO may get involved in include:

a) providing early confirmation of (probable) failure of the approach, sufficient to allow an alternative to be adopted;
b) provide a technical alternative to the original solution with lower risk (risk transformation);
c) the monitoring of project documentation to provide (early) alert to the project if there is evidence that a risk may be instantiating even if it is not declared by the suppliers;
d) monitoring for previously undiscovered risks; and
e) determination that the likelihood of a risk should be lower than previously assessed.

Second pass TRAs involve both an assessment of the current technical risk and an assessment of the implementation of the risk mitigation strategies between first and second pass and whether the technical risks were reduced / retired as expected.

3.11 Identify strategic issues related to the project

There are often key strategic issues associated with the project, and it is useful for the relevant Research Leader and Chief of Division to add on their corporate knowledge in this space. These issues could include long-term DSTO resourcing, future technology trends, implications of the project on other ADF projects and on the ADF system.

4. TRAs in the Capability Development Process

There are different types of TRA that need to be conducted for the Options Review Committee (ORC), First Pass, and Second Pass deliberations[5].

4.1 Preliminary TRA requirements

ORC is about agreeing the capability need and the set of options. The capability development process discussed in [6] includes ORC consideration of a Capability Definition Statement to determine the readiness of the proposal to be included in the DCP. The purpose of the Preliminary TRA is to identify high risk options and mitigation strategies and identify any high risk high payoff options. The Preliminary TRA is a supporting document to the Statement, and:

1. is based on a recognition that the context of use will probably be poorly defined;

2. includes a description of the preliminary system, system boundary, and possibly cross-boundary flows;

3. includes a high-level description of the sub-systems;

4. includes a high-level description of candidate technologies, including high-risk high-payoff technologies;

5. includes a list of which DSTO Divisions (and other areas) should be involved in supporting the project and assessing the technical risks;

6. includes a high-level description of the maturity of the technologies (expressed as TRLs where appropriate); and

7. includes an assessment of the technologies with HIGH technical risk and work that needs to be conducted both prior to first pass (to raise the TRL) and leading to a second pass decision. This could include consideration of CTDs (Capability Technology Demonstrators).

A Preliminary TRA provides Director General Planning and Guidance (DGPG) - the DSTO member at ORC - with the opportunity to shape the direction of the project and scope the DSTO contribution. Since there is a need to undertake broad consultation across DSTO in the identification of candidate technologies, the Preliminary TRA will be signed-off by the Lead Chief of Division.

---

[5] CDS the formal responsibility [1] for defining the technical risk to Government at first pass and second pass. However, by conducting a preliminary TRA for ORC, DSTO has a great opportunity to influence the scope and direction for both the Project and DSTO's work program.

4.2 First Pass TRA requirements

A First Pass TRA is mandated by the DPR process and is signed off by the relevant Lead DSTO Chief of Division. The technical risk is certified by CDS before a Cabinet Submission.

The requirement for a first pass TRA includes:

1. establish the "context of use" from the OCD and FPS;
2. identify the system boundary;
3. identify the key sub-systems for each option;
4. identify the technologies which need to be delivered for each sub-system to work;
5. identify which DSTO divisions (and other areas) should be involved in supporting the project and assessing the technical risks;
6. evaluate the maturity of each technology, expressing the answers as TRLs;
7. identify the set of candidate technical risks for the project;
8. assess the technical risks for the project for each option; and
9. identify possible risk mitigation strategies, particularly for work between first and second pass, and their likelihood for mitigating the risk.

4.3 Second Pass TRA requirements

A Second Pass TRA is mandated by the DPR process and is signed off by the relevant Lead DSTO Chief of Division. The technical risk is certified by CDS before a Cabinet Submission.

There are two major differences between the first and second pass technical risk assessments. The first difference is the quality of technical information and the ability to make assessments about SRLs. The Project S&T Adviser needs to be part of the tender evaluation process to gain access to the technical data from the potential contractors required to conduct a quality second pass TRA.

The second difference is that an assessment needs to be made as to whether the risk mitigation strategies identified at first pass were implemented and, if so, did they successfully reduce or retire technical risk.

The requirement for a second pass technical risk assessment includes:

1. establish the "context of use" from the OCD and FPS;
2. identify the system boundary;

3. identify the key sub-systems;

4. identify the technologies which need to be delivered for each sub-system to work;

5. identify which DSTO divisions (and other areas) should be involved in supporting the project and assessing the technical risks;

6. evaluate the maturity of each technology in terms of TRLs from the tender data;

7. evaluate the maturity of each sub-system in terms of SRLs from the tender data;

8. identify the set of candidate technical risks for the project;

9. assess the technical risks for the project from the tender data;

10. identify possible risk mitigation strategies and their likelihood for mitigating the risk; and

11. document the high technical risks from the first pass TRA, whether the risk mitigation activities were conducted, if so did they successfully reduce / retire the risk, and describe the current level of technical risk.

5. Relating Technical Risk to Studies

DSTO conducts a range of studies to support projects. Examples of studies include: high-level OR studies, detailed OR studies, technology reviews, crewing studies etc.

Developing a TRA may utilise the results of these studies. The relevant studies should be documented in Section 6 of the TRA.

There is a feedback loop from the TRA to the studies. This feedback loop may include[6]:

- The technical risks identify may raise issues or identify critical sub-systems for further sensitivity analysis in the OR studies; and

- The assumptions for the OR studies should align with the technology specifications in the TRA. Where there is a difference, there may be a requirement to examine the implications of the difference on the OA study findings.

Having identified the technical risks in the TRA, the studies may also be used to prioritise the relative importance of the technical risks based on their impact on operational performance (as described in the OCD and FPS). In this manner, the overall

[6] The AIR6000 Phase 2A/2B TRA documented the specifications for JSF (in the form of an ORD) as they were understood at that time. If these specifications change, then DSTO will be able to examine the implications of these changes for both the TRA and the supporting OA studies.

risk assessment table presented in section xx of the TRA would no longer just represent a list of technical risks, it would now represent a prioritised list of technical risks for the project.

6. Summary

This paper has improved the guidance for the conduct of TRAs to address the weaknesses identified in a review of the TRAs certified by CDS. Particular emphasis has been placed on improving the ability to identify and assess SRLs, and the ability to identify and assess technical risks.

References

1. 'Defence Procurement Review 2003'; Malcolm Kinnaird, Len Early, and Bill Schofield; 15 August 2003.

2. 'A Code of Best Practice to Maximise the Contribution of Science and Technology to Acquisition Projects'; DSTO-TR-1743; Joanne Nicholson and Alan Duus; July 2005.

3. 'Technical Risk Assessment: Principles, Process and Procedures', DSTO-GD-0405, Terry Moon, Jim Smith, Joanne Nicholson, Suzanne Fewell and Alan Duus; August 2004.

4. 'Technical Risk Assessment of Australian Defence Projects'; Jim Smith, Graeme Egglestone, Paul Farr, Terry Moon, David Saunders, Peter Shoubridge, Kym Thalassoudis and Tony Wallace; DSTO-TR-1656; December 2004.

5. 'Overview of Capability Development and the Role of Project S&T Plans', John O'Neill and Alan Duus; DSTO-TR-1820; March 2006.

6. 'Defence Capability Development Manual 2005'.

7. 'Changes in DSTO Support to Projects Arising from the 6th July 2006 DCIC Decisions: Updated Guidance for Project S&T Plans'; DSTO-GD-0494, John O'Neill and Alan Duus; 2007.

Page classification: UNCLASSIFIED

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE	3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)
Technical Risk Assessment:: a Practitioner's Guide	Document (U) Title (U) Abstract (U)
4. AUTHOR(S)	5. CORPORATE AUTHOR
John O'Neill, Nitin Thakur and Al Duus	DSTO Defence Science and Technology Organisation PO Box 1500 Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-GD-0493	AR-013-822	General Document	February 2007

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
eg: 510/207/0128	STR 04/254	DCPP	999	999

13. URL on the World Wide Web	14. RELEASE AUTHORITY
http://www.dsto.defence.gov.au/corporate/reports/DSTO-GD-0493.pdf	Chief, Defence Systems Analysis Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DEFTEST DESCRIPTORS

capability assessment, science and technology advice

19. ABSTRACT

DSTO's formal process of preparing Technical Risk Assessments for Acquisition Projects has been in operation for about two years. A recent review of current practices used in the preparation of these assessments identified strengths and weaknesses in the current approach, particularly in the consideration of System Readiness Levels. Remedies to address these weaknesses are addressed in this paper, partly through the development of extensive series of questions designed to assist in the preparation of assessments. The use of Operations Research techniques to determine the operational capability implications of technical risks is also advocated, partly to contribute to a discussion of relative importance of any risk mitigation or risk management strategies.

Page classification: UNCLASSIFIED